# Shifting Regulatory Regimes: From Market Liberalisation to Risk Governance and Data Maximisation

*Simona Stockreiter*

*Summary*

The aim of this analysis is to trace the development of EU data governance over the past approximately thirty years. To map these developments, the analysis divides EU data governance into three phases, each characterised by distinct features. Each phase is defined by one or more regulatory regimes. A regulatory regime is understood here as the constellation of its historical context, regulatory principles and instruments, regulatory narratives, and prevailing conceptions of risk. The analysis seeks to address the following questions: *How does EU data governance respond to increasing regulatory challenges? Which regulatory goals are prioritised in each phase, and how are different regulatory approaches reconciled within individual legal frameworks? Which regulatory narratives and risk perceptions are dominant?* The central hypothesis of this analysis is that the evolution of data governance – contrary to conventional assumptions – is characterised by increasingly pronounced tensions and conflicts between different regulatory goals.

## *1. Introduction*

EU data governance has undergone major developmental shifts over the past thirty years, driven by profound historical and economic transformations associated with the evolution of digital technologies. To trace these developments, this analysis divides EU data governance into three phases, each characterised by distinct features.

The first phase is marked by the Data Protection Directive – the EU's first data protection law. The second phase begins with the GDPR, which constitutes the cornerstone of this period. The third phase starts with the

von der Leyen Commission and is characterised by its new data strategy and the AI Act – the EU's first law regulating artificial intelligence. This three-phase classification is supported by expert interviews as well as a review of the academic literature on the evolution of EU digital policy. While no substantial analyses have yet been conducted specifically on data governance in this context, similar phase-based approaches to the evolution of EU digital governance can be found in the literature.[1]

The aim of this analysis is not only to provide an overview of the development of data governance in the EU over the past approximately thirty years, but also to address, more specifically, the following questions: How does EU data governance respond to increasing regulatory challenges? Which regulatory goals are prioritised in each phase, and how are different regulatory goals reconciled within individual legal frameworks? Which regulatory narratives and risk perceptions are dominant?

The literature on EU digital governance generally assumes a development from a market-opening approach towards an increasingly strong focus on fundamental rights and market-correcting measures.[2] This assumption is examined more closely here with regard to data governance. In contrast to this widespread view of a shift between the goals of EU data policy I argue that both goals remain present in EU data policy and become increasingly conflictual.

In order to facilitate the analysis while ensuring the greatest possible precision, each relevant legal text is examined with regard to its *historical context, regulatory principles*, and *regulatory instruments*. In a second step, the *regulatory narratives*[3] in which each legal text is embedded – and which it reproduces and reinforces – are analysed, together with the *sub-narratives* concerning the perception and communication of *risks*.

Building on this multi-layered approach, the analysis makes visible the extent to which these different dimensions are interlinked. The choice of specific regulatory instruments and the prioritisation of particular princi-

1 See *Savin*, Pravni zapisi 2020, 93.; *Newman*, in: Policy-Making in the European Union, S. 275.; *De Gregorio*, International journal of constitutional law 2021, 41.; *Heidebrecht*, J of Common Market Studies 2023, jcms.13488.

2 See *Savin*, Pravni zapisi 2020, 93.; *Newman*, in: Policy-Making in the European Union, S. 275.; *De Gregorio*, International journal of constitutional law 2021, 41.; *Heidebrecht*, J of Common Market Studies 2023, jcms.13488.; *Bradford*, Digital Empires.

3 The term "narrative" is used interchangeably with "discourse" and "imaginary", since all three refer to shared interpretative frameworks that structure the understanding, communication and legitimisation of technological developments, regulatory challenges and societal risks within a given policy field.

ples within a legal text shape the dominant narratives of a policy field and, ultimately, influence how risks are perceived and communicated at the societal and individual levels – and vice versa. At the same time, tensions may arise between these layers. Prevailing narratives can hence often be traced back to the dominant regulatory instruments and principles underpinning a given framework; when these instruments and principles are themselves in conflict, such tensions could be reflected and amplified in the narratives that accompany them. Finally, it is assumed that changes in the chosen regulatory approach – including shifts in instruments or principles – can in turn alter or reconfigure the dominant narratives of a policy field.

Accordingly, the analysis is based on a qualitative content analysis of the relevant legal texts. In addition, six expert interviews were conducted, which were carried out primarily with senior officials of the EU institutions, as well as with experts active within the Brussels-based EU policy community. They serve mainly to contextualise the regulatory environment and to deepen the understanding of the prevailing regulatory narratives.

## *2. The First Phase of EU Data Governance: A Market-Liberal Orientation?*

The corner stone and starting point of the first phase of EU data governance is the Data Protection Directive (DPD)[4]. Formally adopted in 1995, it constituted the foundational legal instrument for data protection within the EU and served as a principal reference framework for data protection at the global level.

Its development can be traced back to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, as well as the Council of Europe's 1981 Convention No. 108, both of which imposed obligations on entities processing personal data, established a set of individual rights, and underscored that certain categories of sensitive data should be subject to specific legal safeguards. Particularly in light of the increasing fragmentation of national data protection laws in the years that followed, the European Commission decided to introduce a unified European data protection law. The drafting of this legislation took place within the Commission's Directorate-General (DG) for the Internal Market, under the leadership of the centrist-liberal Commissioner *Mario Monti*.

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The directive's dual objectives are set out in Article 1, which states:

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph1.

It thus serves a dual purpose: on the one hand, the protection of a fundamental right, and on the other, the removal of obstacles to facilitate cross-border data transfers within the EU.

The two central regulatory principles underpinning the directive are the *principle of transparency* and the *principle of individual data control*.

The former is operationalised, for instance, through the data subject's right to information and the right of access.[5] More broadly, transparency is a cornerstone of data processing regulation, as it constitutes a necessary precondition for fostering *trust* among data subjects and enables affected individuals to effectively exercise and enforce their data protection rights.[6]

The latter – individual control – is reflected in several provisions, including the right to request the rectification, erasure, or blocking of data, particularly in cases of inaccuracy.[7] It also manifests in the fact that data subjects are granted the right not to be subjected to decisions based solely on automated processing that produce legal effects or similarly significant consequences, such as evaluations of work performance, creditworthiness, reliability, or personal conduct.[8] Furthermore, for personal data processing to be lawful, it must, under certain circumstances, be based on the data subject's consent.[9]

5 The recitals illustrate this point clearly. For example, Recital 38 states that: „the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection" (Data Protection Directive, Recital 38).

6 See *De Hert/Papakonstantinou*, SSRN Journal 2011, (139).

7 Data Protection Directive, Art. 12. In addition, the directive provides for (3) the *right to object* to processing, either where it is unlawful or where it is conducted for the purposes of direct marketing.

8 Data Protection Directive, Art. 15.

9 Data Protection Directive, Art. 7.

With regard to the regulatory instruments, it is notable that, as a *directive* rather than a regulation, the DPD did not establish a fully harmonised regulatory framework that would obligate Member States to adopt identical legal provisions.[10] Instead, it allowed for significant national discretion in implementation.[11] Moreover, the directive was characterised by *weak enforcement mechanisms*. In addition, it promoted various *codes of conduct*, further reflecting a reliance on *soft-law instruments* and *self-regulatory approaches* rather than binding and centralised enforcement.

Overall, it can be concluded that although the first article of the directive sets out two regulatory objectives – a market-oriented goal on the one hand and a fundamental rights objective on the other – no genuine balance was achieved between them. Its primary aim appears to be, first and foremost, the harmonisation of national legislation and the provision of legal certainty to facilitate the creation of a single internal digital market. This is evident from the fact that the directive's legal basis is Article 114 TFEU, which permits legislative action to approximate national laws only insofar as such measures pursue the objective of establishing and ensuring the functioning of the internal market.[12] It is further reflected in the regulatory instruments (e. g. the absence of harmonised enforcement), and in the regulatory principles, in which the principle of individual data control – although granted a significant role – could have been further developed. This reading is also confirmed by relevant CJEU rulings[13] and supported by a number of expert interviews.[14]

The direction taken by this directive can also be understood in the context of a regulatory environment dominated by narratives of *deregulation and market liberalisation*.[15] The prevailing imaginary at the time, as one interviewee described it, was: "You don't have to do anything; the delicate

10 See *Bygrave*, Data privacy law.
11 See *De Hert/Papakonstantinou*, SSRN Journal 2011.
12 *Lynskey*, The foundations of EU data protection law, S. 58.
13 However, the Court's rulings underwent a shift when, with the entry into force of the Lisbon Treaty in 2009, data protection was elevated to a constitutional level within the EU legal order (See *Lynskey*, The foundations of EU data protection law).
14 As one data protection expert observes: "*The Data Protection Directive was heavily market oriented. Its core aim was to harmonise fragmented national rules to facilitate cross-border data flows within the single market. Fundamental rights were mentioned but often subordinated to economic integration, with weak enforcement showing the primacy of market.*" (Interview 3, Senior Expert at EDRi).
15 Interview 2, Senior Official.

plant that is the internet needs time to grow first."[16] These narratives were both reproduced and reinforced by the directive itself. They are also reflected in the associated risk narratives. The primary objective was to foster citizens' *trust* as a prerequisite for market growth.[17] However, another independent narrative that was particularly prominent during the establishment of the DPD was the fear that the state might misuse personal data for totalitarian purposes.[18] In both cases, the focus was less on protecting the individual as such, and more on safeguarding systemic interests – either the smooth functioning of the internal market or the prevention of excessive state power – rather than on establishing strong, enforceable individual rights.

A similar situation applies to the ePrivacy Directive,[19] which was enacted seven years after the adoption of the DPD in 2002. Its objective was to complement the DPD by introducing sector-specific provisions tailored to the unique characteristics of the digital communications environment, such as email services, messaging applications and social networking platforms.

One of the key shortcomings addressed by the ePrivacy Directive was the relatively underdeveloped principle of individual data control that had persisted under the DPD. To remedy this, the ePrivacy Directive introduced a number of specific consent mechanisms, referring for instance to tracking cookies. It established the requirement that users must be informed when a website uses cookies, be provided with clear information on how the data will be used, and be given a meaningful opportunity to accept or refuse such usage.[20]

At the same time, the recitals emphasised that these measures were necessary to strengthen public *trust*, with the aim of facilitating the successful cross-border development of digital networks.[21] Furthermore, the directive highlighted that its harmonization efforts should be limited to what is necessary to ensure that the development and promotion of new

16 Interview 2, Senior Official.
17 Interview 3, Senior Expert at EDRi.
18 Interview 1, Senior Official.
19 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
20 See ePrivacy Directive, Recital 25.
21 It is stated for instance that "the successful cross-border development of [digital networks] is partly dependent on the confidence of users that their privacy will not be at risk". (ePrivacy Directive, Recital 5).

electronic communication services and networks across Member States are not impeded.[22]

In conclusion, the first phase of EU data governance was primarily characterised by the regulatory principles of *transparency* and *individual data control*. At the same time, however, it was also marked by a strong market-oriented focus, particularly on opening up markets and facilitating cross-border data flows. More broadly, the regulatory narrative in the area of data governance during this phase was shaped by a *predominantly technocratic* – as data protection was mostly traded as a technical issue – and *economic discourse*.

### 3. The Second Phase of EU Data Governance: A New Focus on Fundamental Rights?

The second phase of EU data governance is primarily defined by the development and adoption of the 2016 GDPR,[23] which can be regarded as the global cornerstone of data protection regulation. As one senior official put it: "The GDPR was the culmination of the defence of fundamental rights in law."[24]

In contrast to the DPD, the GDPR was drafted within the Commission's DG JUST under the leadership of Viviane Reding, who belonged to the conservative political camp. The proposal was subjected to intense lobbying, resulting in the weakening of several provisions. It was only the Snowden revelations of 2013 that marked a decisive turning point in the drafting process: the disclosures elevated data protection from a technical matter to a politically charged issue. They undermined the public perception of technology companies as neutral service providers, instead casting them as enablers of state surveillance. This "wake-up call"[25] produced a "noticeable shift in the negotiating dynamic".[26] As one senior official recalled:

22 ePrivacy Directive, Recital 8.

23 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

24 Interview 2, Senior Official.

25 Interview 2, Senior Official.

26 *Laurer/Seidl*, Policy & Internet 2021, 257 (13); *Kalyanpur/Newman*, J of Common Market Studies 2019, 448 (453–54).

"We fought like lions, and it was only thanks to Edward Snowden that the regulation came into being. Without Edward Snowden, the resistance and acts of sabotage would have been too great – we would not have succeeded."[27]

The regulatory goals and principles are clearly rooted in the DPD. Like its predecessor, the GDPR is based on two core objectives: a market-making aim on the one hand, and the protection of fundamental rights on the other, as stipulated in Article 1:

*Article 1(2) GDPR:* "The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data."[28]

*Article 1(3) GDPR:* "The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[29]

However, the regulation differs significantly from its predecessor in that it is no longer based on the market-oriented Article 114 TFEU, but instead on Article 16 TFEU, which establishes the fundamental right to the protection of personal data. This legal basis did not exist at the time of the adoption of the DPD in 1995; rather, it was introduced later with the entry into force of the Lisbon Treaty in 2009, alongside Article 8 of the EU Charter of Fundamental Rights (Charter), which likewise enshrines the right to data protection. This means, for example, that the GDPR no longer has to aim at the realization of the four freedoms of the internal market,[30] and that in GDPR-related cases, the CJEU can refer directly to Article 16 TFEU and the Charter.[31]

In terms of regulatory principles, the most prominent under the GDPR are the *principles of transparency, individual data control*, and the newly introduced *principle of accountability*. The first two are significantly strengthened under the regulation: The *principle of transparency* is enhanced through obligations such as the requirement to notify data subjects in the event of data breaches, as well as the obligation for data controllers to main-

27 Interview 2, Senior Official.
28 GDPR, Art. 1(2).
29 GDPR, Art. 1(3).
30 Interview 1, Senior Official.
31 See *Lynskey*, The foundations of EU data protection law.

tain comprehensive records of data processing activities.[32] The *principle of individual data control* is reinforced, for example, through the introduction of the "right to be forgotten"[33] and the strengthening of the right not to be subject to decisions based solely on automated processing, including profiling. This now includes the data subject's rights to obtain human intervention, to express their point of view, and to contest the decision.[34] Additionally, the GDPR introduced new individual rights to compel supervisory authorities to take action, the right to lodge a complaint in cases of inaction, and the right to bring civil proceedings directly against data controllers.[35]

The *principle of accountability*, described by a senior official as a "true novelty",[36] is reflected in several key provisions of the GDPR. These include the principles of data protection by design and by default,[37] the mandatory conduct of Data Protection Impact Assessments (DPIAs) for high-risk processing activities – conducted by the data controllers themselves – and the requirement for them to implement appropriate mitigation measures when such risks are identified. Additionally, in certain cases, the designation of a Data Protection Officer (DPO) is obligatory.[38] In essence, the new principle of accountability means that data controllers are no longer only required to comply with the law – they must also be able to demonstrate that they are in compliance with the regulation.

Among the most important newly introduced regulatory instruments are not only the *DPIAs and DPOs*, but also the *significantly expanded powers of supervisory authorities*, most notably reflected in the introduction of harmonized fines of up to €20 million or 4% of global annual turnover.[39] Moreover, the GDPR takes the form of a *regulation* rather than a directive, thereby eliminating the wide scope for national divergence in implementation that had existed under the previous legal framework.[40]

32 This requirement is planned to be weakened and reduced to cases of "high-risk" processing only under the GDPR "simplification proposal" (as of 01/12/2025).
33 GDPR, Art. 17.
34 GDPR, Art. 22.
35 GDPR, Arts. 77-79.
36 Interview 1, Senior Official.
37 GDPR, Art. 25.
38 GDPR, Art.37.
39 GDPR, Art. 83.
40 As a regulation, the GDPR is directly applicable in all member states and does not require national transposition, thereby significantly reducing fragmentation and

In addition, the regulation integrates two distinct regulatory approaches through its chosen regulatory instruments: a *rights-based approach* and a *risk-based approach*. On the one hand, the GDPR is firmly rooted in constitutional values (particularly Article 8 of the Charter and Article 16 TFEU) which underpin its strong rights-based orientation. On the other hand, this approach is complemented by a risk-based perspective, although the two can exist in a certain degree of tension. The latter is reflected in provisions such as DPIAs, security measures that must be tailored to the level of risk identified by data controllers, and data breach notification requirements, which apply only when a data breach is likely to result in a high risk to individuals' rights and freedoms. The risk-based approach is seen to enhance regulatory flexibility by avoiding a "one-size-fits-all" model[41] and is often portrayed as a tool for promoting competitiveness.[42] However, because it delegates significant regulatory discretion to data controllers, it has been subject to criticism from data protection advocates. As one interviewee noted:

> "The risk-based approach can help prioritize resources, but it sits uneasily with a rights-based framework. Risk assessments often shift responsibility into controllers and can lead to superficial compliance exercises. In contrast, the rights-based approach demands strict observance regardless of risk levels."[43]

Yet, since the risk-based approach in the GDPR can only be regarded as complementary to the rights-based approach – which remains predominant – the prevailing risk narratives focus primarily on the "harm to individual rights and freedoms".[44] The emphasis is placed clearly more strongly than in the DPD on the data subjects' *responsibility* and *autonomy*, as well as on the conceptualisation of *the individual as a holder of fundamental rights*.

This emphasis on individual autonomy and responsibility – understood both as a form of freedom and as a burden – is reflected in specific rights, as repeatedly highlighted in one expert interview:

---

ensuring a higher degree of uniformity compared to the previous directive-based framework.

41 Interview 1, Senior Official.

42 Interview 3, Senior Expert at EDRi.

43 Interview 3, Senior Expert at EDRi.

44 Interview 3, Senior Expert at EDRi.

> "Under the GDPR the citizen can file a complaint with a supervisory authority, which is then obliged to act; if the authority fails to do so, the individual can seek judicial remedy. Furthermore, individuals can initiate legal proceedings directly against companies for data protection violations without needing to rely on the authority's involvement."[45]

This focus also entails a "*subjectivity of risk*," which one senior official critically described as follows:

> "The risk in the GDPR was very subjective, it was linked to how the data subject would understand this risk and therefore all the emphasis was the possibility for the data subjects to exercise their rights, irrespective of any other consideration. The data subject is the ultimate assessor of the risk."[46]

In addition to the risk narratives centered on the individual and their fundamental right to data protection – which inherently involve a strongly subjective component – two further dominant narratives emerged in the context of the GDPR. First, the framing of tech companies as "*enablers of state surveillance*", which became a highly salient political issue following the Snowden revelations. Second, the narrative of the GDPR as a "*golden standard*", that is, a benchmark which has been adopted not only by states on a global level but also by individual non-European tech companies.[47]

Around the same time, however, a kind of counter-movement within EU data governance began to emerge. It started with the 2015 Services Directive[48] and continued with the 2018 Regulation on the Free Flow of Non-Personal Data[49] and the 2019 Open Data Directive.[50] The main regulatory objective of these initiatives was to facilitate the free movement of financial, non-personal, and public-sector data across the EU in order to

45 Interview 2, Senior Official.
46 Interview 1, Senior Official.
47 See *Bradford*, The Brussels effect.
48 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)."2366 - EN - Payment Services Directive - EUR-Lex" 20252366 - EN - Payment Services Directive - EUR-Lex.
49 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance).
50 Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast).

promote competitiveness and data-driven innovation. The respective legal approaches thus exhibited a strong market orientation.

The dominant regulatory principles are *openness* ("open data"), *transparency* (ensured through various recommended codes of conduct, public registers, and similar mechanisms), *efficiency*, and *security*. The regulatory instruments are defined by a series of recommended *technical standards*, as well as by consistently applied – albeit differently weighted – *risk-based approaches*.

One senior official characterized their regulatory imaginary as shaped by "*neo-liberal discourses*".[51] Ultimately, they concluded, it represents a "*neo-liberal counter-movement*".[52] With regard to narratives surrounding risks, one could argue that the predominant focus was on *security threats*. Another interviewee notes critically that risks were understood merely as *barriers to innovation*, and that the overarching objective of these legal frameworks – concerned primarily with risk mitigation – was to build *trust* among companies, member states, and citizens, thereby ensuring the free flow of data across sectors throughout the EU.[53]

In summary, the second phase of EU data governance is primarily characterized by the GDPR's regulatory principles of *individual data control, accountability,* and *transparency*. The regulatory instruments are defined by a *combination of rights-based and risk-based approaches*, with the former taking precedence. As a result, no strong tension exists between the two; rather, they function in a complementary manner. The parallel regulatory trend within data governance during this second phase, however, embodies regulatory principles that in part conflict with those of the GDPR – for example, *individual data control vs. openness*. The regulatory narratives likewise diverge, most notably with regard to their respective focal points: the *protection of individual fundamental rights* on the one hand, and the *emphasis on security risks* with the aim of building *trust* on the other.

Thus, emerging tensions can be observed between differing regulatory principles, instruments, and narratives. At their core, these tensions can be understood as a conflict between a rights-protection orientation and market-making objectives.[54]

51 Interview 2, Senior Official.
52 Interview 2, Senior Official.
53 Interview 3, Senior Expert at EDRi.
54 The Commission has recently announced an "Omnibus" simplification initiative that may adjust certain administrative and reporting obligations under the GDPR as part

### 4. The Third Phase of EU Data Governance: A Shift Towards Broader Societal Harms?

In the third phase – beginning with the first von der Leyen Commission – these tensions intensify due to increasing regulatory complexity. This becomes evident both within individual regulatory frameworks and in the interactions between different pieces of legislation.

On the one hand, the regulatory framework competing with the GDPR continued with the adoption of the Data Governance Act (DGA)[55] and the Data Act (DA).[56] The former, adopted in 2022, constitutes a horizontal regime governing the re-use of certain categories of protected data held by public-sector bodies. Key conditions for such re-use include the consent of data subjects, the requirement that personal data be anonymized (although concrete guidelines on anonymization are lacking[57]), as well as interoperability measures.

In contrast to previous digital policy legislation, this regulation also aims to create new markets. Specifically, it mandates the provision of data intermediation services.[58] These services constitute a new ecosystem designed to connect data holders (supply) with data users (demand). Functioning as neutral data marketplaces, they therefore handle personal and commercially confidential data, with the goal of facilitating the sharing and re-use of certain categories of protected data.[59]

In addition, the regulation encourages the establishment of data altruism organisations,[60] through which both organisations and individual data subjects can voluntarily share their data. The intention is to operationalize the concept of data altruism for the general public interest. Ultimately, these

---

of a broader competitiveness agenda. While the core rights-based architecture of the Regulation remains formally untouched, the initiative illustrates the continuing tension between fundamental-rights protection and market-oriented objectives within EU data governance.

55 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).

56 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance).

57 Interview 4, Senior Official.

58 Data Governance Act, Art. 10-15.

59 Interview 4, Senior Official.

60 Data Governance Act, Art. 16-19.

organisations and individual data subjects decide to whom the data is – or may be – made available, without any specific criteria or allocation guidelines being prescribed by the legislation.

The main regulatory principles of the DGA are *openness, efficiency,* and *security*. The regulatory instruments include *technical standards* as well as a *risk-based approach*. The overarching regulatory objective of the regulation is the creation of a borderless digital internal market. As one senior official put it, "the goal was to make as much data as possible available for sharing",[61] and another interviewee concluded: "it's really about opening up markets".[62] A second aim alongside the internal market objective is to strengthen Europe's position in the global data economy, thereby enhancing the EU's competitiveness.

Regarding the narratives surrounding the regulation, the imaginary of "*data as a resource*" and the paradigm of "*data maximization*" are particularly prominent.[63] One senior official critically observed, in relation to the accompanying risk narratives, that "*rights are seen as implicitly dispensable*".[64] Another noted: "*risks are framed as barriers to innovation and data reuse*".[65]

The Data Act, by contrast, aims to grant data subjects access to data – primarily industrial and IoT data – generated through the use of products or services and held by the data holder (typically the manufacturer). For example, under the DA, the owners of a café may obtain access to the usage data generated by their AI-enabled coffee machine. This data could then be shared with third parties for the development of an application, or used directly by the owner to drive innovation and increase efficiency. In general, the focus of this regulation lies on B2B data sharing. One of the central conditions for enabling such sharing is the principle of data protection by design and by default.

The main regulatory principles include *transparency, efficiency, security*, as well as the principle of *fairness in the data economy* – encapsulated in the notion that "*I control the data on my devices*".[66] In addition, the key regulatory instruments include, besides the principle of *data protection by*

61 Interview 4, Senior Official.
62 Interview 4, Senior Official.
63 See Interview 3, Senior Expert at EDRi.
64 Interview 2, Senior Official.
65 Interview 3, Senior Expert at EDRi.
66 Interview 4, Senior Official.

*design and by default*, the adoption of *technical standards*, and a *risk-based approach*.

The regulatory goals consist in *strengthening the free flow of data within the internal market*, fostering *data-driven innovation*, and positioning the EU as a *global leader in the data-agile economy*. In addition, the regulation aims to *enhance user empowerment*.

Both regulations emerged, as one senior official explained, in response to the fourth industrial revolution and to the realisation that the EU needed to keep pace with the digital economy and become more competitive. As they emphasised, Europe required "a strategy for data that goes beyond the protection of personal data, that goes beyond the fundamental rights approach. Now data is an essential issue not only for democracy and fundamental rights but also for competitiveness [mentioning the Draghi Report]."[67]

Against this backdrop, two interviewees warned – speaking from a critical perspective on the two regulations – that the GDPR's rights-based approach might be undermined by the increasing emphasis on a risk-based or market-oriented rationale for data governance.[68] One interviewee in particular criticised that "the DA and the DGA shift the paradigm towards data maximization to serve industrial and competitiveness goals. This risks undermining GDPR principles of purpose limitation, data minimization and individual control, as well as the ePrivacy Directive."[69]

On the other hand stands the AI Act[70] – the first horizontal legislation in the EU to regulate AI systems, and in general the world's first comprehensive AI law – which was developed in the context of the von der Leyen Commission's agenda strategy "Europe fit for the Digital Age"[71] and the resulting policy programme "EU Digital Decade".[72]

The regulation was adopted in 2024 and developed within DG CNCT (which is frequently criticised for its market-oriented orientation), under

67 Interview 1, Senior Official.
68 Interview 2, Senior Official, Interview 3, Senior Expert at EDRi.
69 Interview 3, Senior Expert at EDRi.
70 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance).
71 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_en (last accessed 15.08.2023).
72 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (last accessed 15.08.2023).

the leadership of Thierry Breton, European Commissioner for the Internal Market, who belongs to the centrist-liberal political camp. It represents an extremely complex attempt to reconcile different regulatory goals. These goals include the protection against physical harms (e. g., self-driving cars crashing), individual harms (e. g., predictive policing), collective harms (e. g., systematised bias), and societal harms (e. g., remote biometric identification), as well as the support of innovation and the development of human-centric AI. Newly introduced, therefore, are regulatory aims concerned with protecting against broader collective and societal harms.[73]

In order to integrate these diverse objectives, the regulation adopts a risk-based approach. Different applications of AI systems are classified within a hierarchy consisting of four risk categories: At the top of this pyramid are unacceptable risks, followed by high risks, limited risks, and minimal risks. In addition, the final version of the AI Act introduced specific requirements for General Purpose AI (GPAI) Models. These latter chapters (Title IV and Title V) include, among other provisions, (minimal) transparency obligations and apply to approximately 80% of AI systems circulating in the EU.[74]

At the top of the pyramid are AI applications considered a "threat to EU values," referring for instance to "real-time" remote biometric identification systems or China-style social credit scoring.[75] High-risk AI systems constitute the core of the regulation and refer to applications that present clear potential risks but are nevertheless deemed manageable. These include the use of AI systems in law enforcement; the administration of justice and democratic processes; education; employment and worker management; healthcare; the management and operation of critical infrastructure; access to and enjoyment of essential private and public services and benefits; and migration, asylum, and border-control management.[76] This represents a wide range of application areas, many of which concern the public sector. One example related to AI in employment is the deployment of automated hiring systems, including tools for emotion recognition designed to evaluate whether an applicant appears happy or nervous while completing a task.

73 See Aritifical Intelligence Act, Article 1.
74 *Stockreiter*, University of Vienna Law Review 2025, 140.
75 Art 5, Aritifical Intelligence Act (Title II).
76 Aritifical Intelligence Act, Annex III.

The condition for authorising high-risk AI systems is that those, regulated under the *product safety regime* – and therefore defined as "products" –, are subject to a specific set of requirements and obligations. Only once these have been met may such systems obtain access to the EU market. These requirements include, for example, that the AI systems rely on high-quality training datasets, meaning that the data must be relevant, representative, and free of errors, and that human oversight is ensured when the system is used.[77]

Because AI is framed as a product and regulated under product legislation, and because the AI Act follows a risk-based approach, a range of *self-assessment mechanisms* plays an important role among the regulatory instruments: EU harmonised standards constitute the cornerstone of product legislation, which means that the European standardisation bodies (CEN and CENELEC) face the challenge of translating high-level, general requirements concerning high-risk AI systems into *concrete technical standards*.[78] In the next step, manufacturers and conformity assessment bodies must evaluate *whether the products comply with these technical product-safety standards*. If this is the case, the systems are authorised to circulate freely within the internal market.

In addition to these procedures, several further self-assessments are required. These include *assessments concerning the classification of AI systems as high-risk*, which enable manufacturers to determine whether their AI system does not fall under the high-risk category;[79] *fundamental rights impact assessments*, which deployers of high-risk AI systems operating in the context of public service provision must conduct;[80] and *GPAI risk*

77 Aritifical Intelligence Act, Arts 9–15.

78 This already gives rise to a number of challenges. In the case of the AI Act, some of the decisions that must be made are highly normative in nature. Standardisation bodies, when developing these standards, need to determine "*how to bring ethics into AI*" – for example, by deciding what constitutes fair and representative datasets for algorithms, by defining transparency guidelines, or by determining the appropriate extent of human control. The decisions taken in this context are all the more contentious because EU standard-setting bodies are "*independent institutions*" that are not directly accountable to democratic political pressures; moreover, member states and the European Parliament have no veto powers. And although mechanisms exist for the inclusion of civil-society actors, they do not possess any formal decision-making authority. See *Veale/Borgesius*, 16.

79 Aritifical Intelligence Act, Art 6 2a-2b.

80 Aritifical Intelligence Act, Art 29a.

*assessments*, as GPAI models with systemic risks are required, among other obligations, to self-assess and mitigate potential systemic risks.[81]

High-risk AI systems are therefore regulated in the context of *pure market surveillance*, as has been the case in previous frameworks for the technical safety of products. This implies not only a set of regulatory challenges, but also that *there are no individual enforcement mechanisms for citizens comparable to those available under the GDPR.*[82]

At the same time, the regulation foresees *substantial administrative fines for non-compliance*. For violations involving prohibited AI practices, fines may reach up to EUR 35 million or 7% of the total worldwide annual turnover of the preceding financial year (whichever is higher).[83] For violations concerning high-risk AI systems – such as non-compliance with the requirements set out in Title III – the AI Act provides for fines of up to EUR 15 million or 3% of the total worldwide annual turnover (whichever is higher).[84]

With regard to the regulatory principles, the principles of *(product) safety, accountability, openness*, and *efficiency* are paramount. In particular, the principles of *safety*, *openness*, and *efficiency* partly conflict with the GDPR principle of *individual data control* – for example, in cases involving remote biometric identification or workplace surveillance. Moreover, these principles are at times balanced against the principle of *transparency*, which, in contrast to earlier regulatory frameworks, occupies a comparatively limited role in the AI Act.

The dominant narratives underpinning the regulation – and significantly reinforced by it, particularly through its choice of regulatory instruments and principles – relate, first, to narratives related to *risk and safety*. As one interview partner critically emphasised multiple times, "*this regulatory regime is organised according to risk and safety*".[85] Second, narratives centred on *competitiveness, jobs, and market growth* are prominent, promot-

81 Aritifical Intelligence Act, Art 52.

82 Interview 2, Senior Official. It can be noted that the AI Act does not create a system of directly enforceable individual rights comparable to the GDPR; however, national remedies and complaints to market surveillance authorities remain available.

83 Aritifical Intelligence Act, Art. 71.

84 Aritifical Intelligence Act, Art. 71. Moreover, a provider of a GPAI models can be subject to potential fines of up to 3% of its total worldwide turnover in the preceding financial year or 15 million EUR, whichever is higher (Art 72a, Aritifical Intelligence Act (Title X)).

85 Interview 5, Senior Official.

ing a "*sense of inevitability*"[86] regarding AI and its manifold applications. Third, narratives concerning *"fundamental questions of the common good"* – questions of *"how technology should be integrated into our lifeworld in the future"*[87]– remain in the background, while *technology-specific narratives* dominate. Hence, although one of the regulatory goals is the protection from collective and fundamental societal harms, there is scarcely any narrative addressing these issues. One reason for this may be that the chosen regulatory instruments and principles do not allow such discourses to emerge; instead, they further reinforce *technocentric narratives*. This reveals a tension between certain regulatory goals and the regulatory instruments and principles, a tension with far-reaching consequences.

With regard to risk narratives, it can further be concluded – as one interviewee critically observed – that although the regulation places a focus on systemic risks, this focus is "operationalised in ways that legitimise many harmful practices"[88]. Another interview partner emphasised critically that "The focus is on product criticism and risk management rather than on the democratic shaping of our future"[89].

Against this backdrop, another interviewee criticised that the dominant narrative around technical risks normalises the AI systems' application and thus renders their *use* unquestioned:

> This approach proposes the idea that as long as you can mitigate some technical risks, then the problems are solved (…) as long as you place some kind of technical means of debiasing, human oversight measures etc. into the system, then everything seems fine. But we should be more critical about what kind of systems we actually accept as maybe a society to be used.[90]

A further interview partner, who welcomes the development that the risk-based approach has become the pillar for digital regulatory approaches, underscores this shift: "The focus has been shifted away from the subjective perspective of the data subject to the product itself. So, it's not so much

86 Interview 5, Senior Official.
87 Interview 2, Senior Official.
88 Interview 3, Senior Expert at EDRi.
89 Interview 2, Senior Official.
90 Interview 6, Mher Hakobyan, Advocacy Advisor on AI Regulation at Amnesty International.

what you or I or the data subject or user may think about it (…) This has to do with a massive historical and economic shift."[91]

In summary, the third phase of EU data governance can be characterised by profound regulatory challenges arising from the attempt to reconcile diverse regulatory goals within complex and comprehensive regulatory frameworks. In this process, tensions emerge even *within* individual frameworks – as illustrated most clearly by the AI Act – between regulatory goals on the one hand and regulatory instruments, principles, and the associated predominant narratives on the other. A closer examination of the AI Act ultimately suggests that objectives related to innovation, internal market harmonisation, and competitiveness take precedence, even though goals such as the protection of fundamental rights and protection against collective and societal harms are formally accorded significant importance.

Furthermore, with regard to regulatory instruments, the third phase is characterised by the widespread use of risk-based approaches, the growing importance of technical standards, and – at least in the case of the AI Act – the introduction of strong enforcement mechanisms. In terms of regulatory principles, the principle of transparency appears comparatively weak when contrasted with earlier phases, while the principle of fairness (as reflected in the Data Act) is newly introduced, and the principle of accountability (as embedded in the AI Act) is strengthened to a certain extent.

## *5. Conclusion*

As a conclusion to this analysis of the shifts in data governance over the past thirty years, it can be shown that there has been no clear linear development – as might be assumed at first glance – from a market-liberal regulatory approach in the first phase, to a fundamental-rights-oriented framework in the second phase, and finally to a focus on protection against collective and fundamental societal harms in the third phase. Such an assumption might arise from a selective focus on particular regulatory goals within specific regulatory frameworks. Rather, the analysis reveals increasingly pronounced conflicts arising from a growing number of regulatory objectives that must be reconciled, but which are in part mutually contradictory.

91 Interview 1, Senior Official

More specifically, these conflicts emerge between the market-opening regulatory goal – which has been present from the outset – and objectives such as the protection of fundamental rights and the protection against broader societal harms, which have progressively moved to the forefront of EU data governance. The growing prominence of these latter objectives has led to increasingly intense tensions within the regulatory framework.

Tab. 1 is intended to illustrate both these fault lines and the continuity of the market-opening objective across all phases. It highlights, for example, the tensions between the principles of data control and openness in the second and third phases, as well as the conflict in the third phase between a risk-based market-surveillance approach and the objective of protecting against systemic and societal harms.

In the third phase, one might even draw the more radical conclusion – based on the prevailing regulatory instruments and principles – that these conflicts are, to a certain extent, resolved in favour of market-oriented regulatory objectives. Yet this need not necessarily be the case. As the GDPR demonstrates, a risk-based approach can complement a rights-based framework, thereby allowing for regulatory flexibility while maintaining the protection of individual fundamental rights at its core. Through a deliberate combination of regulatory instruments and principles, it would also be possible to open up broader, more publicly salient, and more future-oriented narratives. If, for instance, the principal regulatory instruments of the AI Act were not confined primarily to market surveillance mechanisms, criticism of artificial intelligence would no longer be reduced to product safety concerns alone. Instead, the legitimacy of AI deployment could become the subject of broader democratic deliberation. Such a shift would bring narratives concerning societal and systemic harms more prominently to the forefront.

A broader examination of the evolution of narratives within EU data governance reveals that narratives aligned with the market-opening objective have occupied a dominant position from the outset: beginning with data protection framed as a largely technical subject embedded within an economic and market-liberal discourse (Phase I), evolving into narratives centred on competitiveness, data-driven innovation, and data maximisation (Phase II & III), and culminating in predominantly technocratic and technocentric narratives of "risk management" (Phase III). Influential exceptions can be found in the rights-based narratives surrounding the GDPR (Phase II) and, to some extent, in the increased attention to societal harms within the AI Act (Phase III). Nevertheless, a predominance of market-oriented and

technocratic narratives has shaped the subjective experience of citizens, often manifesting in a limited awareness of the broader risks inherent in contemporary data governance and, in some cases, in feelings of powerlessness and resignation vis-à-vis ongoing technological developments. Ultimately, this trajectory underscores the importance of rethinking regulatory design as a means of reshaping the narratives through which digital transformation is collectively understood and democratically negotiated.

*Table 1: The evolution of EU data governance*

| **Regulatory Framweork** | **Phase I: DPD, ePrivacy Directive** | **Phase II: GDPR** | **Phase II: Regulation on the Free Flow of non-personal Data , Open Data Directive, Payment Services Directive** | **Phase III: DA, DGA** | **Phase III: AI Act** |
|---|---|---|---|---|---|
| **Regulatory Principles** | – Transparency<br>– Data control | – Transparency<br>– Data control<br>– Accountability | – Openness<br>– Transparency<br>– Efficiency<br>– Security | – Openness<br>– Efficiency<br>– Security<br>– Fairness | – (Product) Safety<br>– Efficiency<br>– Openness<br>– Accountability |
| **Regulatory Instruments** | – Directive | – Regulation<br>– **Rights-based approach**<br>– Risk-based approach | – **Risk-based approach**<br>– Technical Standards | – Regulation<br>– **Risk-based approach**<br>– Technical Standards | – Regulation<br>– **Risk-based approach**<br>– **Market surveillance**<br>– Technical Standards |
| **Regulatory Objective** | – **Market opening** | – **Stronger tension between fundamental rights protection and market-making objectives**<br>– Importance of data control | – **Market opening** | – **Market opening** | – Protection from **systemic harms**<br>– **Market opening** |
| **Regulatory Narrative** | – Data protection as a technical subject<br>– Economic discourse | – New focus on risks to fundamental right of data protection<br>– highly salient political issue (Snowden revelations)<br>– tech companies as "enablers of sate surveillance"<br>– GDPR as "the golden standard" | – "neo-liberal countermovement" | – Industrial policy<br>– EU's position in the global data economy | – "It's more about risk management than responsibility for the future" |
| **Risk Narrative** | – Protection from state intervention<br>– **Building trust** | – **Focus on harm to individual rights and freedoms**<br>– "subjective risk"<br>– Individual empowerment | – **Focus on security risks**<br>– **Risks as barriers to innovation**<br>– Building trust | – **Focus on security risks**<br>– **Risks as barriers to innovation**<br>– Building trust | – Targets **systemic risks**<br>– **Focus on technical risks**<br>– **Product criticism** |

## List of Interviews

- Interview 1: Senior Official (Online, 30.07.2025)
- Interview 2: Senior Official (Online, 03.09.2025)
- Interview 3: Senior Expert at EDRi (Online, 03.09.2025)
- Interview 4: Senior Official, European Institutions (Online, 25.03.2024)
- Interview 5: Senior Official, European Institutions (Brussels, 01.06.2023)
- Interview 6: Mher Hakobyan, Advocacy Advisor on AI Regulation, Amnesty International (Online, 26.07.2023)

## Literature

*Bradford, Anu*, The Brussels effect: how the European Union rules the world, First issued as an Oxford University Press paperback , New York 2021.

*Bradford, Anu*, Digital Empires: The Global Battle to Regulate Technology, 1 , 2023.

*Bygrave, Lee Andrew*, Data privacy law: an international perspective, Oxford 2014.

*De Gregorio, Giovanni*, The rise of digital constitutionalism in the European Union, International journal of constitutional law 2021, 41–70.

*De Hert, Paul/ Papakonstantinou, Vagelis*, The Proposed Data Protection Regulation Replacing Directive 95/46/Ec: A Sound System for the Protection of Individuals, SSRN Journal 2011.

*Heidebrecht, Sebastian*, From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance, J of Common Market Studies 2023, jcms.13488.

*Kalyanpur, Nikhil/ Newman, Abraham L.*, The MNC-Coalition Paradox: Issue Salience, Foreign Firms and the General Data Protection Regulation, J of Common Market Studies 2019, 448–467.

*Laurer, Moritz/ Seidl, Timo*, Regulating the European Data-Driven Economy: A Case Study on the General Data Protection Regulation, Policy & Internet 2021, 257–277.

*Lynskey, Orla*, The foundations of EU data protection law, Oxford, GB 2015.

*Newman, Abraham L.*, 12. Digital Policy-Making in the European Union: Building the New Economy of an Information Society, in: Policy-Making in the European Union, 2020, 275–296.

*Savin, Andrej*, New directions in EU digital regulation post-2015: Regulating disruption, Pravni zapisi 2020, 93–120.

*Stockreiter, Simona*, The "Governance Turn" in EU Digital Policy, University of Vienna Law Review 2025, 140–168.

*Veale, Michael/ Borgesius, Frederik Zuiderveen*, Demystifying the Draft EU Artificial Intelligence Act, 16.

*Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 1995.

*Directive 2002/58/EC* of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 2002.

*Directive (EU) 2015/2366* of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), OJ L 2015.

*Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 2016.

*Regulation (EU) 2018/1807* of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance.), OJ L 2018.

*Directive (EU) 2019/1024* of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 2019.

*Regulation (EU) 2022/868* of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance), OJ L 2022.

*Regulation (EU) 2023/2854* of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance), 2023.

*Regulation (EU) 2024/1689* of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance), 2024.

## *Über die Autorin*

Simona Stockreiter
promoviert an der Hertie School und ist angebunden am Jacques Delors Centre.
E-Mail: s.stockreiter@phd.hertie-school.org